UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/548,728	04/13/2000	Michael A. Epstein	PHA 23,671	7174

24737 7590 03/08/2004

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
QUINONES, EDEL H	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 03/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/548,728	Applicant(s) EPSTEIN, MICHAEL A.B	
	Examiner Edel H Quinones	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 April 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

III. Detailed Action

Response to Amendment

1. This Office Action is responsive to the amendment filed on February 3, 2004.

Response to Arguments

Applicants arguments have been fully considered by they are moot in view of the new ground(s) of rejection.

The Applicant acknowledges that both check-in/check-out systems and challenge-response protocols are common in the art.

However, the Applicant argues that in the claimed invention, the challenge is provided concurrently with the copy of the content material without regard to a response to the challenge and that the response to the challenge is provided when the content material is returned from the receiving device.

This configuration, however, is analogous to an authentication token, in the form of a challenge-response protocol, and the concept of an authentication token is old and well known in the art.

Drawings

2. The drawings were received on 4/13/2000. These drawings are acceptable.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1, 6 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S Patent 5,251,315 to Wang in view of U.S Patent 5,935,246 to Benson in further view of U.S Patent 4,890,323 to Beker et al.

In regards to claim 1, Wang discloses a method of recreating object/documents in a shared library. This invention provides a "COPY" command that permits the specification of at least three different copy options using the same command. The simple copy option provides for the creation of a new object in a target library using an existing object in a source library in a single unit of work. The check-out option allows an object to be checked out of a source library and copied to a target library. A lock is placed on the object checked out from the source library to prevent changes to it while it is checked out. The check-in option allows an object to be placed in a target library that had been previously checked out and placed in a source library. The check-in option also permits the copy of the object originally placed in the source library to be optionally deleted after the check-in operation is completed (column 2, lines 5-21).

Wang, however, does not disclose that the system communicates a security challenge to the receiving device when the copy of the content material is communicated to the receiving device and that it receives a security response, based on the security challenge, from the receiving device when the copy of the content material is removed from the receiving device.

Benson teaches the use of a challenge-response protocol. Benson discloses a computer system comprising a copy protection mechanism for protecting software against copying, the copy protection mechanism comprising challenge means associated with a protected item of software, and response means in which a customer's private keying material is securely stored (column 3, lines 34-40). Benson teaches that the challenge means comprises means for verifying signed information received from a customer, using the customer's public keying material, and for prohibiting the customer from using some or all items of software unless this verification is successful (column 3, lines 48-52).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made, to have employed the teachings of Benson within the system of Wang, because by using a challenge-response protocol, as taught by Benson, it would have been possible to verify the identity of the receiving device.

The combination of Benson and Wang, however, does not disclose that the challenge is provided concurrently with the copy of the content material and that the response to the challenge is provided when the content material is returned from the receiving device.

The concept of sending a response along with a message in a challenge-response system is old and well known in the art as shown by Beker. Beker teaches a system that provides a response to a challenge in a challenge-response system when the content material (i.e. message) is returned from the receiving device (see Abstract).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Benson and Wang with the teachings of Beker to include providing a challenge concurrently with a copy of the content material and a response to the

challenge when the content material is returned from the receiving device with the motivation to improve the security of transactions flowing across a communication network (see Beker, col. 1, lines 7-9).

In regards to claim 6, Wang discloses a check-out/check-in device comprising a catalog controller configured to provide a limited number of simultaneous copies of content material to one or more receiving devices. This comes in the form of a storage device (figure 1, element 20) which may serve as remote storage for a Local Area Network (LAN) (column 3, lines 1-2). This library, when implemented using DIA structures, is capable of being accessed flexibly and simultaneously by a plurality of users and therefore represents a common repository or shared resource (column 3, lines 45-48). Unlike the shared library, a user's personal or private documents are stored in a local resource (figure 1, element 14). This local storage resource is usually not shared with other users (column 3, lines 49-52). One or more such storage devices may be utilized, in accordance with the method of the invention, to store application or resource objects which may be periodically accessed by any within the data processing system (column 2, lines 53-57). The method of the invention, as discussed for claim 1 above, implements a check-in/check-out system.

The system of Wang, however, does not include an encrypter configured to provide a security challenge to a receiving device when the catalog controller provides a copy of the content material to the receiving device, a receiving device configured to provide a security response based on the security challenge, and a return verifier configured to receive a security response from the receiving device when the copy of the content material is removed from the

receiving device, and to notify the catalog controller whether the security response corresponds to the security challenge.

Benson discloses a computer system comprising a copy protection mechanism for protecting software against copying, the copy protection mechanism comprising challenge means associated with a protected item of software, and response means in which a customer's private keying material is securely stored (column 3, lines 34-40). The system of Benson comprises a cryptographic engine (figure 2, element 21), and a challenge mechanism (figure 2, element 24). The challenge mechanism is configured to generate an unguessable nonce (random number) and to pass the nonce to the signature server with a signature request (column 5, lines46-49). When it receives the signed nonce, the challenge mechanism accesses the keyfile associated with the protected software and calls a signature validation function in the challenge mechanism to validate the vendor's signature of the keyfike, using the vendor's public keying material that is embedded in the challenge mechanism (column 5, lines 60-65). Benson also teaches that the challenge means comprises means for verifying signed information received from a customer, using the customer's public keying material, and for prohibiting the customer from using some or all items of software unless this verification is successful (column 3, lines 48-52).

Therefore, this challenge mechanism serves both as an encrypter configured to provide a security challenge to a receiving device, and a return verifier configured to receive a response for a receiving device and to notify whether the security response corresponds to an appropriate response to the security challenger.

The signature server uses the cryptographic engine to sign the nonce using the customer's private keying material. The signature server then returns the signed nonce to the challenge

mechanism in the protected software (column 5, line 54-59). In other words, the signature server (i.e. receiving device of this system) is configured to communicate a security response based on the security challenge provided by the challenge mechanism.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made, to have employed the teachings of Benson within the system of Wang, because by adding a challenge mechanism serving as an encrypter, a receiving device configured to provide a security response based on the security challenge, and a return verifier configured to receive a security response from the receiving device and to notify the catalog controller whether the security response corresponds to the security challenge, as taught by Benson, it would have been possible to verify the identify of the receiving device and to prevent a receiving device from receiving content material unless this verification is successful.

The combination of Benson and Wang, however, does not disclose that the challenge is provided concurrently with the copy of the content material and that the response to the challenge is provided when the content material is returned from the receiving device.

The concept of sending a response along with a message in a challenge-response system is old and well known in the art as shown by Beker. Beker teaches a system that provides a response to a challenge in a challenge-response system when the content material (i.e. message) is returned from the receiving device (see Abstract).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Benson and Wang with the teachings of Beker to include providing a challenge concurrently with a copy of the content material and a response to the challenge when the content material is returned from the receiving device with the motivation to

improve the security of transactions flowing across a communication network (see Beker, col. 1, lines 7-9).

In regards to claim 11, Wang discloses a check-out/check-in device comprising a catalog controller configured to provide a limited number of simultaneous copies of content material to one or more receiving devices. This comes in the form of a storage device (figure 1, element 20) which may serve as remote storage for a Local Area Network (LAN) (column 3, lines 1-2). This library, when implemented using DIA structures, is capable of being accessed flexibly and simultaneously by a plurality of users and therefore represents a common repository or shared resource (column 3, lines 45-48). Unlike the shared library, a user's personal or private documents are stored in a local resource (figure 1, element 14). This local storage resource is usually not shared with other users (column 3, lines 49-52). One or more such storage devices may be utilized, in accordance with the method of the invention, to store application or resource objects which may be periodically accessed by any within the data processing system (column 2, lines 53-57). Such a storage device is interpreted to correspond to the memory configured to store content material and the corresponding security challenge. This security device is assumed to be configured to erase the content material from memory given that this can be one of the steps of the method of the Wang invention.

Wang, however, does not disclose that the receiving device receives a security challenge from the check-out/check-in device and that it communicates a security response to the check-out/check-in device, based on the security challenge.

Benson teaches the use of a challenge-response protocol. Benson discloses a computer system comprising a copy protection mechanism for protecting software against copying, the copy protection mechanism comprising challenge means associated with a protected item of software, and response means in which a customer's private keying material is securely stored (column 3, lines 34-40). Benson teaches that the challenge means comprises means for verifying signed information received from a customer, using the customer's public keying material, and for prohibiting the customer from using some or all items of software unless this verification is successful (column 3, lines 48-52).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made, to have employed the teachings of Benson within the system of Wang, because by using a challenge-response protocol, as taught by Benson, it would have been possible to verify the identity of the receiving device.

The combination of Benson and Wang, however, does not disclose that the challenge is provided concurrently with the copy of the content material and that the response to the challenge is provided when the content material is returned from the receiving device.

The concept of sending a response along with a message in a challenge-response system is old and well known in the art as shown by Beker. Beker teaches a system that provides a response to a challenge in a challenge-response system when the content material (i.e. message) is returned from the receiving device (see Abstract).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Benson and Wang with the teachings of Beker to include providing a challenge concurrently with a copy of the content material and a response to the

challenge when the content material is returned from the receiving device with the motivation to improve the security of transactions flowing across a communication network (see Beker, col. 1, lines 7-9).

2. Claims 2, 4-5, 7, and 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S Patent 5,251,315 to Wang in view of U.S Patent 5,935,246 to Benson in further view of U.S Patent 4,890323 to Beker et al. as applied to claims 1 and 6 above, and further in view of U.S. Patent 5,568,552 to Davis.

The combination as thought by Wang as modified by Benson and Beker, as discussed for claims 1 and 6 above, discloses a check-in/check-out method and device for limiting simultaneous copies of content material, comprising: communicating a copy of the content material to a receiving device, communicating a security challenge to the receiving device when the copy of the content material is communicated to the receiving device, and receiving a security response, based on the security challenge, from the receiving device when the copy of the content material is removed from the receiving device.

In regards to claims 2 and 7, the combination, however, does not include verifying a certification of the receiving device before communicating the copy of the content material to the receiving device.

Davis discloses an apparatus and method for enabling a roving software license to be transferred between appropriately configured hardware agents thereby eliminating the need for a distributable physical hardware device (column 3, lines 48-52). Davis teaches that authentication of the sender (i.e., verifying that the sender of a public key is, in fact, the true owner of the public

key) is a problem when communications are initially established between previously unknown parties. This problem is commonly avoided by incorporating a digital certificate within a transmission message (column 4, lines 66-67 and column 5, lines 1-4).

Referring to Figure 3, upon receipt of the transmission message 50 from the first node 10 being transmitted through the public domain 25, the second node 15 decrypts the SKenc 85 with its private key (CPRK2) 17 and the digital certificate 45 with a published public key ("PUBTA") of the trusted authority 55 to obtain SK 60 and PUK1 11 These SK and PUK1 keys 60 and 11 are used to decrypt the encrypted original message 65 and the digital signature 80 to retrieve the transmitted message digest 75 and the original message 40, respectively. The original message 40 then undergoes a hash algorithm 85, identical to that performed in the first node 10. The results (referred to as a "received message digest") 90 are compared to the transmitted message digest 75. If the transmitted message digest 75 is identical to the received message digest 90, communications are maintained between these legitimate nodes. (column 5, lines 34-49). In other words, the first node communicates a certificate to the second node, and the second node acts as a certification verifier configured to verify a certification of the receiving device, wherein communications are maintained based upon this certification

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made, to have employed the teachings of Davis within the combination of Wang, Benson and Beker, because by using a certificate to verify the receiving device, as taught by Davis, it would have been possible to authenticate the identity of the receiving device when communication was being established between previously unknown parties.

In regards to claims 4 and 9, the combination, however, does not disclose that the system generates a random number, encrypts the random number via a public key of a public-private key pair associated with the receiving device to form a security challenge, and includes the random number in the security response.

Benson discloses that the challenge mechanism of the protected software generates an unguessable nonce (random number) and passes the nonce to the signature server with a signature request. When it receives the nonce, the signature server first checks that the nonce presented to it corresponds exactly to the format FIG 4, with the exception of the 32 random-appearing character. If it does not, the signature server denies the signature request. Assuming that the nonce is in the correct format, the signature server uses the cryptographic engine to sign the nonce using the customer's private keying material. The signature server then returns the signed nonce to the challenge mechanism in the protected software (column 5, lines 46-59). The challenge mechanism uses a random number generator to ensure freshness of the protocol (column 11, lines18-20).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made, to have further applied the teachings of Benson to the aforementioned combination, because generating a random number, sending the random number in a security challenge, and including the random number in the security response, as taught by Benson, is an effective way of ensuring freshness of the challenge-response protocol.

Davis, on the other hand, presents an apparatus and method for enabling a roving software license to be transferred between appropriately configured hardware agents thereby eliminating the need for a distributable physical hardware device (column3, lines 48-52). After

the hardware agent is constructed, it is implemented into an electronic device such as the computer system illustrated in FIG. 4. This is accomplished by establishing a secure communication path between the licenser and the hardware agent through authentication procedures such as challenge/response as well as any other well-known procedures (column 7, lines 63-67, and column 8, lines 1-2). Referring to figure 7A, in Step 225 and 230, using the derived public key of the first hardware agent, the second hardware agent encrypts a challenge message according to a chosen cryptographic algorithm (e.g., RSA) and transmits the challenge message to the first hardware agent. In step 235 and 240, the first hardware agent decrypts the challenge message with its private key ("PRK1") and generates a response message by encrypting the decrypted challenge message with the public key of the second hardware agent ("PUK2") and transmits the response message to the second hardware agent (column 8, lines 31-40).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made, to have modified the combination of Wang, Benson and Beker with the teachings of Davis, because by encrypting the challenge via a public key of a public-private key pair associated with the receiving device, as taught by Davis, it would have been possible to establish a secure communication path.

In regards to claims 5 and 10, the combination, however, does not disclose that the system further verifies a certification of the receiving device before communicating the copy of the content material and that the certification includes a public key of the public-private key pair of the receiving device.

Davis teaches that authentication of the sender (i.e., verifying that the sender of a public key is, in fact, the true owner of the public key) is a problem when communications are initially established between previously unknown parties. This problem is commonly avoided by incorporating a digital certificate within a transmission message (column 4, lines 66-67 and column 5, lines 1-4). Davis also discloses that the authentication device certificate will include at least the public key of the device "digitally signed" with the secret private manufacturing key (i.e. in general terms, encrypting the public key of the device with the manufacturer's private key) (column 7, lines 47-51).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made, to have further applied the teachings of Davis to the combination of Wang, Benson and Beker, because by verifying a certification of the receiving device before communicating the copy of the content material wherein the certification includes a public key of the public-private key pair of the receiving device, as taught by Davis, it would have been possible to authenticate the participating parties.

3. Claims 3 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S Patent 5,251,315 to Wang in view of U.S Patent 5,935,246 to Benson in further view of U.S Patent 4,890323 to Beker et al. as applied to claims 1 and 6 above, and further in view of U.S. Patent 5,754,763 to Bereiter.

In regards to claims 3 and 8, as discussed for claims 1 and 6 above, the combination as thought by Wang as modified by Benson and Beker, discloses a method and device for limiting simultaneous copies of content material, the system comprising: communicating a copy of the

content material to a receiving device, communicating a security challenge to the receiving device when the copy of the content material is communicated to the receiving device, and receiving a security response, based on the security challenge, from the receiving device when the copy of the content material is removed from the receiving device.

The combination, however, does not further disclose that it maintains a count of the simultaneous copies of the content material, including incrementing the count when the copy of the content material is communicated to the receiving device, and decrementing the count when the security response is received from the receiving device, and wherein communicating the copy of the content material is dependent upon the count of the simultaneous copies.

Bereiter presents an invention directed to managing a large distributed computer enterprise environment and, more particularly, to auditing licensed program usage in a manner that does not increase management overhead and that may be carried out without user involvement (column 1, lines 6-10). According to the invention as illustrated in the flowchart of FIG. 7, the managed environment is first organized into a logical "hierarchy" as illustrated in FIG. 1. This is step 100 in the flowchart. At step 102, a system management task is initiated. During the execution of a system management task, an object supported on a first machine (e.g., an endpoint) invokes an object located on a second machine (e.g., a gateway), or vice versa. Method invocations are carried out in a secure manner, using a remote procedure call or some similar mechanism. As a management task is effected, the number of method invocations (for the program being used to carry out the task) is counted at step 104. Conveniently, this count provides a simple way of determining whether an authorized number of software copies (of a particular program) are running in the system. Thus, for example, assume the system

management task in question is carried out using a software application and that the organization (including all endpoints) is licensed to have 500 copies of that application. Upon execution of the system management task that affects all endpoints, the number of method invocations of the software application should equal the number of authorized copies. At step 106 then, a test is made to determine if the number of particular method invocations exceeds the number of authorized copies of the program in question. If the outcome of the test at step 106 is affirmative, then an authorized usage has been located and the routine continues at step 108 to issue a warning to the system administrator. Remedial action may then be taken at step 110. If the outcome of the test at step 106 is negative, then the routine terminates with respect to the particular invocation (column 8, lines 44-67, and column 9, lines 1-7). It is an obvious step in the above method to decrement the counter once a copy of the software stops running.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made, to have employed the teachings of Bereiter within the combination of Wang, Benson and Beker, because by maintaining a count of the simultaneous copies of the content material, including incrementing the count when the copy of the content material is communicated to the receiving device, and decrementing the count when the security response is received from the receiving device, and wherein communicating the copy of the content material is dependent upon the count of the simultaneous copies, as taught by Bereiter, it would have been possible to control the number of copies of the content material being communicated to the receiving devices.

4. Claims 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S Patent 5,251,315 to Wang in view of U.S Patent 5,935,246 to Benson in view of U.S Patent 4,890323 to Beker et al. as applied to claim 11 above, in further view of U.S Patent 5,568,552 to Davis.

The combination as thought by Wang as modified by Benson and Beker, discloses the system of claim 11 as discussed above.

In regards to claim 12, the system of Wang, Benson and Beker, however, does not disclose that the receiving device communicates a certification.

In regards to claim 13, the system of Wang, Benson and Beker, however, does not disclose that the receiving device includes a decrypter that decrypts the security challenge via a private key associated with the receiving device.

In regards to claim 14, the system of Wang, Benson and Beker, however, does not disclose that the certification of the receiving device includes a public key of the public-private key pair of the receiving device

Davis presents an apparatus and method for enabling a roving software license to be transferred between appropriately configured hardware agents thereby eliminating the need for a distributable physical hardware device (column3, lines 48-52). After the hardware agent is constructed, it is implemented into an electronic device such as the computer system illustrated in FIG. 4. This is accomplished by establishing a secure communication path between the licenser and the hardware agent through authentication procedures such as challenge/response as well as any other well-known procedures (column 7, lines 63-67, and column 8, lines 1-2). Referring to figure 7A, in Step 225 and 230, using the derived public key of the first hardware agent, the second hardware agent encrypts a challenge message according to a chosen

cryptographic algorithm (e.g., RSA) and transmits the challenge message to the first hardware agent. In step 235 and 240, the first hardware agent decrypts the challenge message with its private key ("PRK1") and generates a response message by encrypting the decrypted challenge message with the public key of the second hardware agent ("PUK2") and transmits the response message to the second hardware agent (column 8, lines 31-40).

Davis teaches that authentication of the sender (i.e., verifying that the sender of a public key is, in fact, the true owner of the public key) is a problem when communications are initially established between previously unknown parties. This problem is commonly avoided by incorporating a digital certificate within a transmission message (column 4, lines 66-67 and column 5, lines 1-4). Davis also discloses that the authentication device certificate will include at least the public key of the device "digitally signed" with the secret private manufacturing key (i.e. in general terms, encrypting the public key of the device with the manufacturer's private key) (column 7, lines 47-51).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made, to have employed the teachings of Davis within the system of Wang, Benson and Beker because by including a receiving device that decrypted a security challenge via a private key associated with the receiving device, and provided a security response based on the security challenge, and by the receiving device communicating a certification including a public key of the public-private key pair of the receiving device, as taught by Davis, it would have been possible to establish a secure connection and to authenticate the participating parties.

Other Prior Art Made of Record

A. Perlman et al. (U.S. Patent No. 6,173,400) discloses a methods and systems for establishing a shared secret using an authentication token.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Points of Contact

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edel H Quinones whose telephone number is 703-305-8745. The examiner can normally be reached on M-F (8:00AM-5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheik can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Edel H. Quiñones
Patent Examiner
Technology Center 2100
March 3, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100